UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,163	06/28/2001	Robert A. Jerdonek	020967-000220US	7419

20350 7590 04/14/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,163	JERDONEK, ROBERT A.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 2 February 2006 with an original application filed 28 June 2001, and continuing filing date of 17 January 2001.

2. Claims 1-10 and 12-21 are currently pending in this application. Claims 1, 8, and 15 are independent claims.

Response to Arguments

3. Applicant's arguments filed 2 February 2006 have been fully considered but they are moot due to new grounds of rejection.

Specification Objections

4. The disclosure is objected to because of the following informalities: The Related U.S. Application Data only cites Provision application No. 60/262,875, filed on Jan. 17, 2001. This is the same Provision application that U.S. Application No. 09/896,560 now US Patent No. 6,983,381 (hereinafter '381), which was also filed on 28 June 2001 cited. The Application Data needs to indicate that this application is a co-pending divisional application. In additional information and investigation is needed if a Provisional Applications can be divided, and that both inventions contain appropriate disclosure in the Provisional Application. Appropriate correction and information is required.

5. This application appears to be a divisional of Provisional application No. 60/262,875 filed on Jan. 17, 2001, the other application that also references the Provisional Application is 09/896,560 now US Patent No. 6,983,381 (hereinafter '381),

filed 28 June 2001. A later application for a distinct or independent invention, carved out of a pending application and disclosing and claiming only subject matter disclosed in an earlier or parent application is known as a divisional application or "division." The divisional application should set forth the portion of the earlier disclosure that is germane to the invention as claimed in the divisional application.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A statutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-10 and 12-21 are rejected on the ground of statutory obviousness-type double patenting as being unpatentable over claims 1-20 of copending 09/896,560 now US Patent No. 6,983,381 (hereinafter '381). This is a statutory double patenting rejection since the conflicting claims have been patented. Although the conflicting claims are not identical, they are not patentably distinct from each other because an obvious variant of code that directs the processor to request a challenge to verify a password is communication method for providing passwords after receiving a challenge.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-10 and 12-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The independent claims all contain the phrase "via a first secure communications channel" this phrase is indefinite because the word "first" is not followed by the words "second" or "next" etc communications channel.

10. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1-4, 6-10, and 12-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al. U.S. Patent No. 6,952,781 (hereinafter '781) in view of Yatsukawa U.S. Patent No. 6,148,404 (hereinafter '404) in further view of Baskey et al. U.S. Patent No. 6,732,269 (hereinafter '269).

As to dependent claim 1, "A computer program product for a client computing system including a processor includes: code that directs the processor to request" is taught in '781 col. 5, lines 34-41 (note code that directs is interpreted to be equivalent to a daemon);

"a challenge from an authentication server; code that directs the processor to receive the challenge from the authentication server" is shown in '781 col. 7, lines 30-49;

"wherein the challenge includes a at least a password that is inactive" and **"in response to the password that is inactive from the authentication server"** is disclosed in '781 TABLE 2, (note the OTP is expired this is interpreted to be equivalent

to an inactive password, the CHAP password entered and verified is in response to the inactive password);

"code that directs the processor to receive user authentication data from a user" is taught in '781 col. 11, line 40 through col. 12, line 3;

"wherein the authentication server activates the password" is show in TABLE 2;

the following is not taught in '781:

"**code that directs the processor to determine a private key and a digital certificate in response to the user authentication data; code that directs the processor to form a digital signature" and "the private key; code that directs the processor to communicate the digital signature to the authentication server"** however '404 teaches "an authentication method for authenticating an authentication requester by using a public-key enciphering scheme in response" and "According to another aspect of the present invention authentication data is sent to the authentication server together with a public-key certificate" in col. 11, lines 8-39 and col. 13, lines 33-35;

"code that directs the processor to communicate the digital certificate to the authentication server, the digital certificate comprising a public key in an encrypted form and code that directs the processor to communicate network user authentication data and the password that is inactive to the authentication server via a security server" however '404 teaches "In the example shown in FIG. 16, it is a precondition that the server obtains a public-key certificate of the client X at

each log-in. In other words, the client sends the server, for instance, the public-key certificate CK_{px} of the client X along with the authentication data. When the authentication processing program 104 at the server side receives a log-in message of a client X, the program 104 returns an authentication data request message to the client. When the program 14 receives authentication data transmitted by the client X in response to the message, the program 104 inspects a digital signature of the certification authority (CA), which is added to the public-key certificate of the client X, by utilizing a public key K_{pc} (stored in the file 107) of the CA. If the inspection result shows that the digital signature is authentic, the program 104 verifies that the public-key certificate is the authentic public-key certificate of the client X. The public-key certificate $CK._{px}$ of the client X is stored in the inspection data file 105. The deciphering processing program 106 accesses the inspection data file 105 and derives the public key K_{px} of the client X included in the public-key certificate CK.sub.px" in col. 20, lines 11-31;

the following is not taught in '404 and '781: **"via a first secure communication channel"** however '269 teaches "These and other objects of the present invention may be provided by methods, systems, and computer program products which communicate between client applications and a transaction server by establish a persistent secure connection between the transaction server and a Secure Socket Layer (SSL) proxy server" in col. 2, lines 21-40.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '082 method for communicating passwords to

include a means to authenticate a user with public/private keys. One of ordinary skill in the art would have been motivated to perform such a modification to because as network communication improves a need exist to verify an entity utilizing electronic methods. As indicated by '404 (see col. 1, lines 15-32) "For instance, in a case where legal action is taken between business entities or between individuals, conventionally (or even now), a contract or the like is written on a physical document, signed, impressed with a seal, and if necessary, accompanied with a registration certificate of seal impression or a notary certificate by notary officials ... Technology in electronic data communication that safely substitutes the above action taken mostly on physical documents, is the network security technology ... the demands on network security technology are steadily increasing".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '404 a method for authenticating users utilizing public/private key cryptography to include a means to utilize a secure socket layer. One of ordinary skill in the art would have been motivated to perform such a modification to because as network communication improves a need exist to maintain with security communication standards available. As indicated by '269 (see col. 1, lines 13 et seq.) " In communications between a client and a server, it is often beneficial to provide increased security. One mechanism for providing increased security is through the use of the Secure Socket Layer (SSL) protocol. FIG. 1 illustrates a conventional SSL connection between a client 10 and a server 12. As

seen in FIG. 1, the client 10 communicates directly with the server 12 utilizing the SSL connection".

As to dependent claim 2, "wherein the password that is inactive remains inactivate when the authentication server does not verify the digital signature" is disclosed in '404 col. 20, lines 11-31.

As to dependent claim 3, "wherein the security server comprises a server selected from a group consisting of: firewall server, VPN gateway server" is shown in '269 col. 5, lines 38-57 "other forms of secure connection may be utilized, such as, for example, a Virtual Private Network (VPN) tunnel, Internet Protocol Security (IPSEC)".

As to dependent claim 4, **"wherein code that directs the processor to determine the private key and the digital certificate in response to the user authentication data comprises code that directs the processor to determine a private key associated with the user when the user authentication data is correct"** is disclosed in '404 col. 20, lines 11-31.

As to dependent claim 6, **"further comprising code that directs the processor to receive network user authentication data from the user"** is taught in '404 col. 12,

lines 39-67.

As to dependent claim 7, **"wherein code that directs the processor to receive user authentication data from a user comprises code that directs the**

processor to receive user authentication data and the network authentication data from the user" is shown in '404 col. 12, lines 39-67.

As to independent claim 8, "A client computing system for communicating with a private server includes: a tangible memory configured to store a key wallet" is taught in '404 col. 12, lines 39-67

"the key wallet including a private key associated with the user and a digital certificate associated with a user, the private key and digital certificate stored in an encrypted form; a processor coupled to the tangible memory, the processor configured to receive a challenge from an authentication server" and **"configured to receive user authentication data from the user, configured to determine a retrieved private key and a retrieved digital certificate from the key wallet in response to the user authentication data from the user; configured to form a digital signature in response to the password that is inactive from the authentication server and the retrieved private key, configured to communicate the digital signature to the authentication server, configured to communicate the digital certificate to the authentication server, and configured to communicate network user authentication data and the identity code to the authentication server via a security server, wherein the authentication server activates the identity code when the digital signature is verified, and wherein the security server allows the client computing system to communicate with the private server when the password that is inactive is activated" "** is shown in '404 col. 20, lines 11-31;

"the challenge comprising a password that is inactive" is shown in '781 TABLE 2;

"via a first secure communication channel" is disclosed in '269 col. 2, lines 21-40 "These and other objects of the present invention may be provided by methods, systems, and computer program products which communicate between client applications and a transaction server by establish a persistent secure connection between the transaction server and a Secure Socket Layer (SSL) proxy server".

As to dependent claim 9, **"wherein the retrieved private key and the private key associated with the user are identical"** is taught in '404 col. 11, lines 40-50 "the authenticator deciphers the received authentication data sent by the requester by using a public key of the authentication requester, and compares the deciphered data with inspection data ... inspecting whether or not they are coincident".

As to dependent claim 10, **"wherein the retrieved private key and the private key associated with the user are different, and wherein when the retrieved private key and the private key associated with the user are different the identity code remains inactive"** is shown in '404 col. 18, lines 9-21 "Log-in is granted only when the deciphered data coincides with inspection data which has been stored at the authenticator's side. Accordingly, as long as, a client securely keeps his/her own secret key, a third person who has any or all) of the authentication data ... is unable to "masquerade" as the authentic client".

As to dependent claim 12, **"wherein the security server comprises a server selected from a group of servers consisting of: firewall server, VPN gateway server, electronic mail server, web server, database server, database system, application server"** is disclosed in '269 col. 5, lines 38-57.

As to dependent claim 13, **"wherein the tangible memory can be removed from the client computer"** is taught in '404 col. 20, lines 58-63 "Therefore, in the second modified example, the secret key K_s is stored in an IC card instead of the client terminal, enabling the client X to carry around the IC card".

As to dependent claim 14, **"wherein the processor is also configured to receive the network user authentication data from the user"** is shown in '404 col. 12, lines 39-67.

As to independent claim 15, this claim incorporates substantially similar subject matter as claims 1 and 8; therefore it is rejected along the same rationale.

As to dependent claim 16 this claim is substantially similar to claim 9; therefore they are rejected along the same rationale.

As to dependent claim 17, wherein the means for determining a returned private key comprises means for determining the returned private key in response to the PIN from the user, and a pre-determined PIN, wherein when the PIN from the user and the pre-determined PIN are different, the returned private key is different from the private key associated with the user, wherein when the PIN from the user and the pre-determined PIN are the same, the returned private key is the private key associated with the user" is taught in '404 col. 21, lines 11-26 "First, when a user makes a log-in request (e.g. an IC card is read by

a card reader which is not shown), the enciphering processing program 303 sends an authentication data request message (message requesting a password) to the client via the authentication processing program 308 of the terminal. If the user is an authentic user, a correct password is inputted from a keyboard (not shown) of the terminal. When the password is inputted, the program 308 sends the inputted password to the enciphering processing program 303 via interface. The enciphering processing program 303 compares the received password with a password stored in the password file 307. If the passwords do not coincide, the message indicating non-coincidence is returned to the authentication processing program 308, which then rejects the log-in request".

As to dependent claim 20, **"wherein the client computing system is selected from a group of devices consisting of: desktop computer, portable computer, PDA, wireless device"** is shown in '404 col. 21, lines 61-67 " More specifically, the system at the client side may be a general-purpose personal computer, and the personal computer may be used by persons other than the client X. In addition, any terminal can be used as the client's main apparatus as long as the terminal is capable of interfacing with an IC card. Accordingly, for instance, remote log-in or the like using a portable terminal is enabled from outside".

As to dependent claim 21, "wherein the password that is inactive is determined in the authentication serer, and wherein the password that is inactive is not stored on the client computer system before receiving the challenge from the authentication server" is disclosed in '404 col. 13, lines 30-33 "According to

another aspect of the present invention, identification data of the authentication requester is used as an initial value of the first seed data".

As to dependent claim 18, **"further comprising means for receiving at least a network password associated with the user from the user, wherein the means for communicating the digital certificate and the digital signature to the authentication server also comprise means for communicating the network password associated with the user to the authentication server"** is shown in '781 col. col. 4, lines 10-43 "A method and apparatus for validating access to a network system is disclosed ... In response to entering the username and one-time password, a user authorization phase is performed to determine whether a session should be established for the particular user".

As to dependent claim 19, **"wherein the means for communicating the digital certificate and the digital signature to the authentication server also comprise means for communicating a network password associated with the user to the authentication server; the client system further comprising means for determining the network password associated with the user in response to at least the PIN from the user"** is taught in '781col. 4, lines 10-43".

13. **Claim 5,** is rejected under 35 U.S.C. 103(a) as being unpatentable over '781 in view of '404 in further view of '269 in further view of Arthan et al. U.S. Patent No. 6,782,103 (hereinafter '103).

As to dependent claim 5, the following is not taught in '404 and '**269 "wherein code that directs the processor to determine the private key and the digital**

certificate in response to the user authentication data further comprises code that directs the processor to determine a private key not associated with the user when the user authentication data is incorrect" however '103 teaches "If a key becomes compromised, then good cryptographic practice dictates that operational use of that key be suspended. The key then needs to be changed so that business can proceed using new uncompromised key" in col. 3, lines 9-17.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '404 and '269 a method for authenticating users utilizing public/private key cryptography with SSL to include a means to change private key when authentication is incorrect. One of ordinary skill in the art would have been motivated to perform such a modification to because it is good practice to change keys when data becomes compromised. As indicated by '103 (see col. 1, lines 50 et seq.) "Good cryptographic practice requires all keys be changed at regular intervals, but if a key becomes compromised then it needs to be changed at other than the appropriate regular interval".

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
08 April 2006

JAGDISH N. LOUIS-JACQUES
PRIMARY EXAMINER